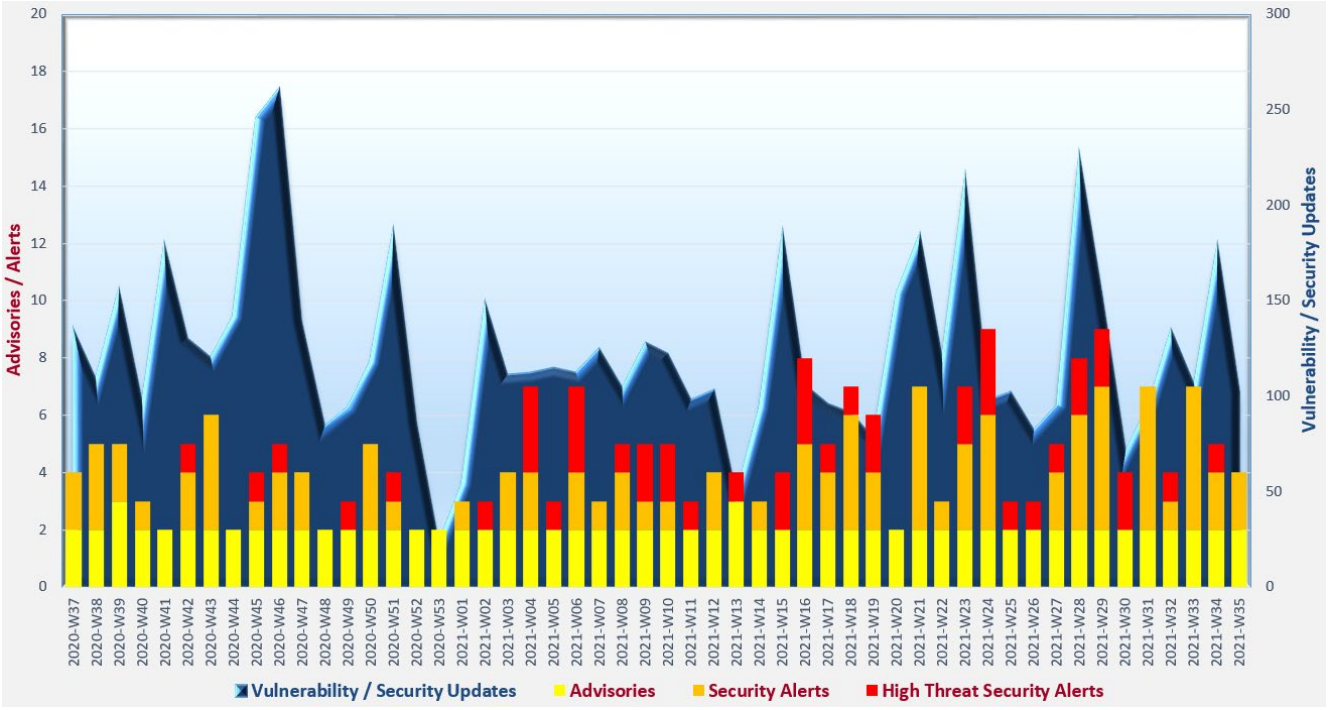
TLP:WHITE

# Cyber Security Threat Trends 2021-M08

August 2021

With reference to the FIRST Traffic Light Protocol (TLP) standard[1], this document is classified as TLP:WHITE information. Recipients may share with peers and partner organisations without restriction.

## Cyber Security Threat Landscape of the past 12 months (source: GovCERT.HK)




**Trending:**

**Phishing attacks** keep growing. Attackers increasingly target to **compromise user credentials**. Users should use different credentials and strong passwords for different websites or e-services, adopt multi-factor authentication if available, and be vigilant on suspicious links and attachments in electronic messages. Organisations should regularly conduct security awareness training to keep their users abreast of updated security policies and new developments in the cyber security threats, trends and defence techniques.

[1] https://www.first.org/tlp/

## CERT Advisories

### Active exploitation of vulnerabilities in various products

CERT bodies issued alerts regarding active exploitation against vulnerabilities in various products. Proof of Concept (PoC) codes for exploitation of some vulnerabilities were publicly available. System administrators should refer to vendors' documentation, apply system patches and perform mitigation measures immediately.

- GovCERT.HK[2], HKCERT[3], JPCERT[4] and MyCERT[5] issued alerts regarding multiple vulnerabilities in Microsoft products. Vulnerability in Microsoft Windows and Windows Server (CVE-2021-36948) was being actively exploited. Successful exploitation could lead to elevation of privilege.

- CERT NZ[6], Australian Cyber Security Centre (ASCS)[7], Cybersecurity and Infrastructure Security Agency (CISA)[8], and Canadian Centre for Cyber Security[9] issued alerts regarding active exploitation targeted ProxyShell vulnerabilities (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207) in Microsoft Exchange Servers. Successful exploitation of these vulnerabilities would allow a remote attacker to execute arbitrary commands on the impacted Exchange servers.

- HKCERT[10] and Canadian Centre for Cyber Security[11] issued alerts regarding a remote code execution vulnerability (CVE-2021-36958) in Windows Print Spooler service. PoC on exploitation of the vulnerability existed. System patch was not yet available at the time of publishing the alert. Workaround measures were provided by the vendor.

- GovCERT.HK[12] and HKCERT[13] issued alerts regarding multiple vulnerabilities in Cisco products. PoC exploit code for the vulnerability CVE-2021-34749 was available.

- Canadian Centre for Cyber Security[14] issued alert regarding vulnerability (CVE-2021-3050) in Palo Alto PAN-OS. Successful exploitation of the vulnerability would allow an attacker to execute arbitrary commands. Exploits for the vulnerability were publicly available.

---

2 https://www.govcert.gov.hk/en/alerts_detail.php?id=628
3 https://www.hkcert.org/security-bulletin/microsoft-monthly-security-update-august-2021
4 https://www.jpcert.or.jp/english/at/2021/at210034.html
5 https://www.mycert.org.my/portal/advisory?id=MA-813.082021
6 https://www.cert.govt.nz/it-specialists/advisories/active-scanning-for-microsoft-exchange-proxyshell-vulnerability/
7 https://www.cyber.gov.au/acsc/view-all-content/alerts/microsoft-exchange-proxyshell-targeting-australia
8 https://us-cert.cisa.gov/ncas/current-activity/2021/08/21/urgent-protect-against-active-exploitation-proxyshell
9 https://www.cyber.gc.ca/en/alerts/ongoing-exploitation-proxyshell-exploit-chain
10 https://www.hkcert.org/security-bulletin/microsoft-windows-remote-code-execution-vulnerability_20210816
11 https://www.cyber.gc.ca/en/alerts/ongoing-vulnerabilities-involving-windows-print-spooler
12 https://www.govcert.gov.hk/en/alerts_detail.php?id=633
13 https://www.hkcert.org/security-bulletin/cisco-products-multiple-vulnerabilities_20210819
14 https://www.cyber.gc.ca/en/alerts/palo-alto-networks-security-advisory-10

## CERT Advisories

### Secure Kubernetes systems

CISA and National Security Agency (NSA) have released Kubernetes Hardening Guidance[15], which provides recommendations in hardening Kubernetes systems on various areas such as Kubernetes Pod security, network separation and hardening, authentication and authorisation, log auditing, etc.

[15] https://us-cert.cisa.gov/ncas/current-activity/2021/08/02/cisa-and-nsa-release-kubernetes-hardening-guidance

## Industry Insight on Cyber Security Threat Trends

**Phishing attacks increased in the first half of 2021**

PhishLabs published the "Quarterly Threat Trends & Intelligence Report"[16], which summarised their analysis on phishing attack trends. The key findings were:

- **The number of phishing sites encountered in the first half of 2021 was 22% higher than the same period last year.** 45% of phishing attacks targeted accounts used for Single Sign-On (SSO). Financial industry was the most targeted industry in Q2 2021, followed by social media and telecommunications.
- **Abuse of free services or tools contributed to 62% of all the phishing sites.** Top three abused services included tunnelling services (24%), free hosting (16.6%) and free domain registrations (11.8%). 27.2% of phishing sites were hosted in compromised sites.
- **63.5% of the phishing emails found in corporate users' inboxes attempted to steal credentials.** Corporate-reported credential theft phish targeting Office 365 credentials increased from 44.5% in Q1 2021 to 51% in Q2 2021.
- **In Q2 2021, 35.3% of phishing emails were sent by free email accounts, increased from 34.3% in Q1 2021.** Gmail was the most commonly used free email domain, accounted for 20.7% of all phishing emails reported in Q2 2021.
- **Phishing attacks on social media rose.** The monthly average number of attacks on social media per organisation in June 2021 was 49.5, a 47% increase from 33.6 in January 2021. Fraud-related social media attack was the most common attacking technique, rose 23.7% as compared to Q1 2021 and accounted for 45.6% of social media attacks in Q2 2021. Payment services was the most targeted industry in social media attacks and recorded an increase of over 5.6 times.

*Source: PhishLabs*

[16] https://info.phishlabs.com/quarterly-threat-trends-and-intelligence-august-2021

## Industry Insight on Cyber Security Threat Trends

**Credential stuffing attack was prominent**

Arkose Labs analysed the traffic and attack patterns in the first half of 2021 and published its "2021 State of Fraud Report"[17]. The key findings were:

- **Fake new account registration increased 70% as compared with the second half of 2020.** More than one-third of attacks detected in the first half of 2021 were fake new account registrations. Peak attack volume reached 43 million attacks in one week. The number of fake account registrations climbed up to 211 million in Q2 2021. Attackers used synthetic or stolen credentials to create fake accounts. Almost 80% of the 100 surveyed IT executives opined that it was difficult to identify new account fraud.

- **285 million credential stuffing attacks were detected, accounted for 29% of all attacks detected and 5% of all analysed network traffic in the first half of 2021.** For instance, gaming industry encountered 225 million credential stuffing attacks. Moreover, 1.5 million credential stuffing attempts targeted a social media network were detected in one week.

- **Mobile attacks increased 40% from the end of 2020.** On average, 24% of attacks detected were launched by mobile devices. Gaming industry encountered the highest mobile attack rate, with 34% of attacks originated from mobile devices.

- **The top three attack origin regions were Asia, followed by Europe and North America, accounted for 34.1%, 29% and 24.7% of attacks in the first half of 2021, respectively.** Asia also had the highest percentage of human fraud farm attacks, using human to supplement automated attacks, or conduct other fraudulent activities that required higher nuance.

*Source: Arkose Labs*

[17] https://www.arkoselabs.com/resource/2021-state-of-fraud-report/

## Industry Insight on Cyber Security Threat Trends

**Outdated operating systems, unpatched vulnerabilities and orphaned accounts were found in connected devices**

Ordr published the "Rise of the Machines 2021: State of Connected devices — IT, IoT, IoMT and OT" [18], which summarised their analysis results on anonymised data from more than 12 million connected devices from June 2020 to June 2021. The key findings were:

- **42% of connected devices were agentless devices.** These agentless devices could not be protected by endpoint security software agents, and were targeted by attackers to serve as entrances to networks for further lateral movement and compromise.
- **Devices were found running outdated operating systems such as Windows CE, Windows XP or Windows 7.** Support on these operating systems ended and security patches were no longer available. Attackers could seize the opportunity to exploit the unpatched vulnerabilities to compromise the devices. For instance, in healthcare industry, 32% of medical imaging devices and 15% of medical devices run on obsolete operating systems.
- **46% of connected devices were susceptible from attacks ranging from medium to high severity.** Over 80% of these attacks were connection to malicious URLs (73.18%) or phishing sites (9.34%).
- **Orphaned accounts or accounts with default or weak password were found in the connected devices.** This could impose risk of compromise of accounts or escalation of user privilege and subsequent lateral movement across the network.
- **Organisations should patch their systems timely, maintain complete visibility of the connected devices, baseline the usage and traffic patterns of the devices, adopt zero trust and least privilege defence approach and network segmentation, and conduct continuous monitoring on their networks.**

*Source: Ordr*

[18] https://resources.ordr.net/reports/rise-of-the-machines-2021#main-content

## Highlight of Microsoft August 2021 Security Updates

| Product Family | Impact[19] | Severity | Associated KB and / or Support Webpages |
|---|---|---|---|
| **Windows 10** | Remote Code Execution | Critical ★★★★ | KB5005030, KB5005031, KB5005033, KB5005040, KB5005043 |
| **Windows 8.1** | Remote Code Execution | Critical ★★★★ | KB5005036, KB5005076, KB5005106 |
| **Windows Server** | Remote Code Execution | Critical ★★★★ | KB5005030, KB5005033, KB5005036, KB5005043, KB5005076, KB5005094, KB5005099, KB5005106 |
| **Microsoft Office-related software** | Spoofing | Important ★★★ | KB4011600, KB5002000, KB5002002 |

Note: Only widely-used Microsoft products are listed and it does not mean to be inclusive. For details, please refer to https://msrc.microsoft.com/update-guide/en-us/releaseNote/2021-Aug.

Learn more:
High Threat Security Alert (A21-08-06): Multiple Vulnerabilities in Microsoft Products (August 2021) (https://www.govcert.gov.hk/en/alerts_detail.php?id=628)



[19] The Impact and Severity are the maximum impact and severity assessment of the vulnerabilities in the associated knowledgebase (KB) by Microsoft.